



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/822,226	04/08/2004	Sumeet Singh	15670-075001/ SD2004-151	1313
20985 7590 10/04/2007 FISH & RICHARDSON, PC P.O. BOX 1022 MINNEAPOLIS, MN 55440-1022			EXAMINER OKORONKWO, CHINWENDU C	
			ART UNIT 2136	PAPER NUMBER
			MAIL DATE 10/04/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/822,226

Applicant(s)

SINGH ET AL.

Examiner

Chinwendu C. Okoronkwo

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 04/08/2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 and 69-79 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-35 and 69-79 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☒ Claim(s) 36-68 and 80-87 are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 21 July 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 20070608.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____.

DETAILED ACTION

Priority

1. For the record, the Examiner acknowledges that no priority claim has been made in regards to this application.

Information Disclosure Statement

2. For the record, the Examiner acknowledges that the IDS submitted on 05/09/2005 and 06/08/2007. It has been received and considered.

Oath/Declaration

3. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 07/12/2004 has been received and considered.

Drawings

4. For the record, the Examiner acknowledges that the Drawings submitted on 04/08/2004 have been received and considered.

Specification

5. For the record, the Examiner acknowledges that the Specification submitted on 04/08/2004 has been received and considered.

Election/Restrictions

6. Restriction to one of the following inventions required under 35 U.S.C 121:
- I. Claims 1-35 and 69-79, drawn to a method for collecting data to be analyzed in order to determine a network attack, classified in class 726, subclass 22-25 and 27-31.
 - II. Claims 36-58 and 80-87, drawn to an apparatus which generates a signature and has a connection to a network and obtains a portion of data from the network operating to carry out a data reduction on said data portion, classified in class 380, subclass 28-30 and 245-246.

Inventions I and II are related as subcombinations disclosed as usable together in a single combination. The subcombinations are distinct if they do not overlap in scope and are not obvious variants, and if it is shown that at least one subcombination is separately usable. In the instant case, subcombination II has separate utility such as the specification of a "signature generator that obtains a portion of data from the network operating to carry out a data reduction on said data portion." See MPEP 806.05(d).

During a telephone conversation with Bing Ai on September 12, 2007 a provisional election was made without traverse to prosecute the invention of Group I, claims 1-35 and 69-79. Affirmation of this election must be made by applicant in replying to this Office action. Claims 36-58 and 80-87 withdrawn from further

Art Unit: 2136

consideration by the examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-6, 11-15, 20-21, 33-35, 69, 71, 75 and 79 and rejected under 35

U.S.C. 102(e) as being disclosed by Cox et al. (US Patent No. 6,738,814 B1).

Regarding claim 1, Cox et al., discloses a method comprising: obtaining a portion of data to be analyzed to determine a network attack and analyzing a plurality of said reduced data portions to detect common elements within said reduced data portion, said analyzing reviewing for common content indicative of a network attack (col. 1 lines 60-67 – “analyzing an incoming data packet from the public network. The incoming data packet is then matched against known forms of attack on the private network”).

Cox et al. is silent in disclosing the carrying out a data reduction on said portion, however it would have been obvious to one of ordinary skill in the

art to modify the disclosed invention to reduce said data portions. This would be obvious to one of ordinary skill in the art because one of ordinary skill would know that the data packets – which by definition are ***reductions of the original data*** (hence the name “packet”) – are better handled and analyzed in smaller portions. Therefore, motivation for this modification would be to allow for the received packet to be properly analyzed.

Regarding claim 2, Cox et al., discloses a method as in claim 1, wherein said analyzing common content comprises determining frequently occurring sections of message information within said reduced data portion (col. 1 lines 60-67 – “analyzing an incoming data packet from the public network. The incoming data packet is then matched against known forms of attack on the private network.”).

Regarding claim 3, Cox et al., discloses a method as in claim 1, wherein said analyzing common content comprises determining increasing number of sources and destinations that are sending and/or receiving within said portions (col. 1 line 67 and col. 2 lines 1-7).

Regarding claim 4, Cox et al., discloses a method as in claim 1, further comprising analyzing for the presence of a specified type of code within said data (col. 1 lines 60-67 – “analyzing an incoming data packet from the public network.

The incoming data packet is then matched against known forms of attack on the private network.”).

Regarding claim 5, Cox et al., discloses a method as in claim 2, further comprising after said analyzing determines said frequently occurring sections of message information, then carrying out an additional test on said frequently occurring sections of message information (col. 3 lines 34-45 – “based upon pattern matching ... the routing device can identify the data packet and its source as malicious or non-malicious”).

Regarding claim 6, Cox et al., discloses a method as in claim 5, wherein said additional test is a test to look for an increasing number of at least one of sources and destinations of said frequently occurring sections of message information (col. 3 lines 54 – “routing device compares the IP address of the packet against known internal IP addresses of the associated private network ... if the source IP address”).

Regarding claim 11, Cox et al., discloses additional test comprising maintaining a first list of unassigned addresses, forming a second list of sources that have sent to addresses on said first list and comparing a current source of a frequently occurring section to said second list (col. 3 lines 54-65).

Regarding claim 12, Cox et al., discloses a method as in claim 11, wherein said maintaining, and said forming, and said comparing, each comprise data reducing information in said first list and said second list (col. 3 lines 54-65).

Regarding claim 13, Cox et al., discloses a method as in claim 5, wherein said additional test comprises: first monitoring a first content sent to a destination; second monitoring a second content sent by said destination; and determining a correlation between said first content and said second content as said additional test (col. 4 lines 1-14).

Regarding claim 14, Cox et al., discloses a method as in claim 13, wherein said first monitoring comprises monitoring multiple destinations, and said second monitoring comprises monitoring multiple destinations during a different time period than said first monitoring (col. 4 lines 15-26).

Regarding claim 15, Cox et al., discloses a method as in claim 14, wherein said first and second monitoring comprises data reducing information about said destinations, and storing at least one table about said data reduced information (col. 4 lines 1-26).

Regarding claim 20, Cox et al., discloses method as in claim 1, further comprising forming a plurality of portions from each network packet, each of said

plurality of portions comprising a specified subset of the network packet
(Rejected under the combined rationales as claim 1).

Regarding claim 21, Cox et al., discloses a method as in claim 1, further comprising forming a plurality of portions from each network packet, each of said plurality of portions comprising a continuous portion of payload, and information indicative of a port number indicating a service requested by a network packet
(Rejected under the combined rationales as claims 11 and 20).

Regarding claim 33, Cox et al., discloses a method as in claim 1, further comprising, determining a list of first computers that are susceptible to a specified attack, and monitoring only messages directed to said first computers for said specified attack (Rejected under the same rationale as claim 1).

Regarding claim 34, Cox et al., discloses a method of claim 33 where said monitoring comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable, as said specified attack (Rejected under the same rationale as claim 1).

Regarding claim 35, Cox et al., discloses a method as in claim 34, wherein said checking comprises checking for a field that is longer than a specified length
(Rejected under the same rationale as claim 1).

Regarding claim 69, Cox et al., discloses a method, comprising: monitoring network content on a network, and obtaining at least a portion of data on said network; data reducing said portion of data using a data reduction function which reduces said portion of data to a reduced data portion in repeatable manner, such that each portion which has the same content is reduced to the same reduced data portion; analyzing said reduced data portion to find network content which repeats a specified number of times, and to establish said network content which repeats said specified number of times as frequent content; identifying address information which includes at least one of a source information or destination information for sources and/or destinations, of said frequent content, and determining if a number of sources and/or destinations for said frequent content is increasing; and identifying the frequent content as associated with a network attack, based on said identifying (Rejected under the same rationale as claim 1).

Regarding claim 71, Cox et al., discloses a method as in claim 70, wherein said obtaining a portion of network data comprises defining a window which samples a first portion of network data at a first time defined by a position of the window, and sliding said window to a second position at a second time which samples a second portion of said network data that has a specified offset from the first portion (Rejected under the same rationale as claim 1).

Regarding claim 75, Cox et al., discloses a method as in claim 69, wherein said identifying comprises second data reducing said address information using a data reduction function, and maintaining a table of data reduced address information (Rejected under the same rationale as claim 1).

Regarding claim 79, Cox et al., discloses a method as in claim 69, further comprising monitoring for scanning of addresses associated with said frequent content (Rejected under the same rationale as claim 11).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 7-9, 16-19, 22-32, 70-74 and 76-78 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cox et al. (US Patent No. 6,738,814 B1) and further in view of Townshend (US Patent No. 6,829,635 B1).

Regarding claim 7, Cox et al., is silent in disclosing a method as in claim 5, wherein said additional test includes a test to look for code or opcode (operation code) within the frequently occurring sections, however it would have been obvious for one of ordinary skill in the art to modify the invention disclosed by Cox into the claimed invention due to disclosure of the comparison between the "requested connection and one or more existing connections (col. 4 lines 29-31)." It would have been obvious because the connection requests are codes to various connection ports. Therefore to look for code or opcode within sections of data is an obvious reference to connection port codes, which Cox does disclose (col. 4 lines 15-39).

Regarding claim 8, Cox et al., is silent in disclosing a method wherein said data reduction includes carrying out a hash function on said portion of data, however Towshend does disclose such hashing in column 6 lines 39-56. It would have been obvious to combine these two inventions and the motivation would be to improve the storage of the patterns disclosed by Cox in column 3 lines 36-39 which recites, "known patterns ... can be built using knowledge about various types of attacks. This knowledge can be recorded in the form of patterns that are then stored in a database or other storage device accessible by the routing device."

Regarding claim 9, Cox et al., does not explicitly disclose a method wherein said determining frequently occurring sections is done by using at least first, second and third data reduction techniques on each said portion, to obtain at least first, second and third results, and to count said first, second and third results, and to establish frequently occurring sections when all of said at least first second and third results have a frequency of occurrence greater than a specified amount, however it would have been obvious for one of ordinary skill in the art to modify the invention disclosed by Cox into the claimed invention due to disclosure of "the routing device [storing] information about the attack for later use and for analysis for administrators of the private network. For example, information concerning the packet origination, destination or content can be stored internally to the router device or sent to a syslog server for later analysis." The motivation here would be that such data stored for analysis and used as claimed would allow the administrators to act more proactively and better filter out data which have potential of causing network attacks (col. 4 lines 9-14).

Further Townshend does disclose determining frequently occurring sections in column 2 lines 11-14. It would have been obvious to combine these two inventions and the motivation would be to improve how proactively the invention behaves and allow for better filtering of data which have potential of causing network attacks

Regarding claim 10, Cox et al., is silent in disclosing a portion of data that at least includes a portion of the network payload, however Towshend does disclose network payload and the signatures disclosed in Townshend are the models used in predicting possible threats to the network, which by definition are what network payloads are. The motivation for the combination is to provide better means of determining the threat level of data being analyzed.

Regarding claim 16, Cox et al., discloses a method as in claim 10, wherein said portion of data further includes portion of a network header (Rejected under the same rationale as claim 10).

Regarding claim 17, Cox et al., discloses a method as in claim 11, wherein said portion of a network header is a port number indicating a service requested by a network packet (Rejected under the same rationale as claim 7).

Regarding claim 18, Cox et al., discloses a method as in claim 17, wherein said port number is a source port or a destination port (Rejected under the same rationale as claim 7).

Regarding claim 19, Cox et al., discloses a method as in claim 1, wherein said portion of data comprises a first subset of a network packet including payload and header and further comprising obtaining a second subset of the same

network packet for subsequent analysis (Rejected under the same rationale as claim 10).

Regarding claim 22, Cox et al., discloses a method as in claim 2, wherein said determining frequently occurring sections comprises: taking a first hash function of said portion, first maintaining a first counter, with a plurality of stages, and incrementing one of said stages based on said first hash function; taking a second hash function of said portion; and second maintaining a second counter, with a plurality of stages, and incrementing one of said stages of said second counter based on said second hash function (Rejected under the combined rationales as claim 8).

Regarding claim 23, Cox et al., discloses a method as in claim 22, further comprising checking said one of said stages of said first counter and said one of said stages of said second counter against a threshold, and identifying said portion as frequent content only when both said one of said stages of said first counter and said one of said stages of said second counter are both above said threshold (Rejected under the same rationale as claim 11).

Regarding claim 24, Cox et al., discloses a method as in claim 23, further comprising adding frequent content to a specified frequent content buffer table

(Rejected under the same rationale as claim 11).

Regarding claim 25, Cox et al., discloses a method as in claim 24, further comprising taking at least a third hash function of said portion, and incrementing a stage of at least the third counter based on said third hash function, where said identifying identify said portion as frequent content only when all of said stages of each of said first, second and third counters are each above said threshold

(Rejected under the same rationale as claim 8).

Regarding claim 26, Cox et al., discloses a method as in claim 22, further comprising obtaining said portion by taking a first part of the message, and subsequently obtaining a new portion by taking a second part of the message
(Rejected under the same rationale as claim 1).

Regarding claim 27, Cox et al., discloses a method as in claim 26, wherein at least one of said hash functions is an incremental hash function (Rejected under the same rationale as claim 8).

Regarding claim 28, Cox et al., discloses a method as in claim 3, wherein said data reduction comprises hashing at least one of the source or destination address, to form a hash value, first determining a unique number of said hash

values, and second determining said one of source or destination numbers based on said first determining (Rejected under the same rationale as claim 8).

Regarding claim 29, Cox et al., discloses a method as in claim 28, wherein said counting further comprises scaling the hash value prior to said second determining (Rejected under the same rationale as claim 8).

Regarding claim 30, Cox et al., discloses a method as in claim 29, wherein said scaling comprises scaling by a first value during a first counting session, and scaling by a second value during a second measurement interval (Rejected under the same rationale as claim 8).

Regarding claim 31, Cox et al., discloses a method as in claim 7, wherein said detecting code comprises looking for a first valid opcode at a first location, based on said first valid opcode, determining a second location representing an offset of said first valid opcode, and looking for a second valid opcode at said second location (Rejected under the same rationale as claim 7).

Regarding claim 32, Cox et al., discloses a method as in claim 31, further comprising establishing the portion as including code when a predetermined number of valid opcodes are found at proper distances (Rejected under the same rationale as claim 7).

Regarding claim 70, Cox et al., discloses a method as in claim 69, wherein said monitoring network content comprises obtaining both a portion of data on the network, and a portnumber indicating a service requested by a network packet (Rejected under the same rationale as claims 17 and 18).

Regarding claim 72, Cox et al., discloses a method as in claim 71, wherein said data reduction function is a hash function (Rejected under the same rationale as claim 8).

Regarding claim 73, Cox et al., discloses a method as in claim 72, wherein said data reduction function is an incremental hash function Rejected under the same rationale as claim 8).

Regarding claim 74, Cox et al., discloses a method as in claim 69, wherein hash function is used in a scalable configuration (Rejected under the same rationale as claim 8).

Regarding claim 76, Cox et al., discloses a method as in claim 75, wherein said second data reducing comprises hashing said address information (Rejected under the same rationale as claim 8).

Regarding claim 77, Cox et al., discloses a method as in claim 69, further comprising testing contents of the network packet associated with the frequent content to determine the presence of code in said contents (Rejected under the same rationale as claim 7).

Regarding claim 78, Cox et al., discloses a method as in claim 77, wherein said testing contents comprises determining an opcode in said contents, determining a length of the opcode, and looking for another opcode at a location within said contents based on said length Rejected under the same rationale as claim 7).

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2136


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



CCO

September 29, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100


9,29,07